REMARKS

I. Introduction

In response to the Office Action dated October 20, 2004, claims 3 and 30 have been cancelled, claims 1, 4, 19-21, and 31 have been amended, and 43-50 have been added. Claims 1, 2, 4-29, 31-50 are in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. The Cited References and the Subject Invention

A. The Akins Reference

U.S. Patent No. 6,560,340, issued May 6, 2003 to Akins, III et al. disclose a method and apparatus for geographically limiting service in a conditional access system. A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

B. Differences Between the Subject Invention and the Cited References

The Akins reference and the Applicants' invention differ in a number of important respects. Most importantly, the Akins reference is directed to a system for providing conditional access to programs based on geographic limitations. It is not directed to the secure storage of media programs at the subscriber's location for later playback. As described below, this substantial

difference explains why selected features of the Applicants' invention may be appear to be present in the Akins reference, but in fact are not, as the features do not interact with other features in the same way, nor do they provide the same functionality.

IV. Office Action Prior Art Rejections

In paragraph (2), the Office Action rejected claims 1-42 under 35 U.S.C. § 102(e) as being anticipated by Akins, III et al., U.S. Patent No. 6,560,340 (Akins). Applicants respectfully traverse these rejections.

With Respect to Claim 1:

Claim 1 recites:

A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;

(b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;

(c) decrypting the program material using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage.

According to the Office Action, step (a) is disclosed as follows:

When the service distribution organization broadcasts an instance of the service, it encrypts or scrambles the instance to form encrypted instance 105. Encrypted instance 105 contains instance data 109, which is the encrypted information making up the program, and entitlement control messages (ECM) 107. The entitlement control messages contain information needed to decrypt the encrypted portion of the associated instance data 109. (col. 4, lines 26-33)

The Office Action also suggests that steps (b)-(f) are disclosed as follows:

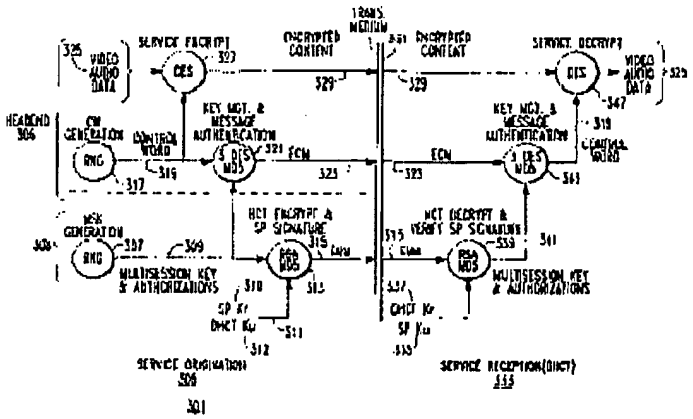
In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1.sup.st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is

called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208). (col. 6, lines 24-54)

However, both of the foregoing passages refer to the process wherein the head end generates a control word (CW) and uses that control word to encrypt the media program before it is sent to the subscriber … essentially .. to operations that take place *before* step (a) of claim 1.

Recall that claim 1 requires that the program material that was accepted in step (a), and decrypted in step (c) is the same program material that is re-encrypted in step (d). Both of the above passages refer to the encryption of the program material. Neither of them refer to re-encrypting the material according to a second key, encrypting the second key according to a third key to produce a fourth encryption key, and providing the re-encrypted material and the fourth encryption key for storage.

The Applicants note that the Akins reference does disclose encrypting program material with a key and encrypting they key as well, for example in FIG. 3 below:



The Applicants also note that the Akins reference discloses storing the encrypted program material and the encrypted encryption key as follows:

> .... Also, the transmission medium may be storage media, where the service origination point is the manufacturer of the media, and the service reception component may be the element which reads the storage media. For example, the transmission medium can be a CD-ROM, DVD, floppy disk, or any other medium that can be transferred, physically, electronically, or otherwise. (col. 7, lines 49-55)

... but that storage is a form of transmitting the program material to the viewer ... it is an alternative to the step of receiving data stream transmitted from the head end. Not surprisingly then, this process does not disclose steps (a)-(c) ... the step of receiving encrypted program material and decrypting it.

Finally, Claim 1 has been amended to recite that the encryption of the second encryption key according to a third encryption key to produce a fourth encryption key is performed in a *conditional access module releasably coupleable with the receiver*, the *same* conditional access module that is used to decrypt the encrypted access control information.

Similar features were recited in (now canceled) claims 3 and 4. The Office Action argued that the features of claim 3 were disclosed in col. 6, lines 24-53 (reproduced above), and that the features of claim 4 are disclosed in the following passage:

> DHCTSE 627 includes a microprocessor (capable of performing DES), specialized hardware for performing RSA encryption and decryption, and secure memory elements. All of the components of DHCTSE 627 are contained in a single tamper-proof package, such as a package that upon attempting to access the information contained within the information is destroyed. Only the components of DHCTSE 627 have access to the information stored in the secure memory elements. Any attempt by a user to gain access to any of the parts of DHCTSE 627 renders DHCTSE 627 unusable and its contents unreadable. DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a "smart card". The user "personalizes" the DHCT 333 by installing the module in it. (col. 21, lines 1-14)

True enough, the foregoing discloses a removable element (which may be a smartcard) having encryption and decryption elements. However, the *DHCTSE* does not *encrypt a second encryption key according to a third encryption key to produce a fourth encryption key*. If these functions are performed at all in the Akins reference at all, they are performed by the headend before the media program is sent to the subscriber, not afterwards ... and hence, cannot be performed by the DHCTSE.

The Applicant has reviewed the rather lengthy Akins disclosure and cannot ascertain any passage that might reasonably be interpreted as using an conditional access module that is releasably coupleable with the receiver to perform these functions. Rather, the encryption capabilities of the DHCTSE appear to be used for securing transmissions from the subscriber to the head end:

> FIG. 4 also shows how the techniques used to ensure the security of EMMs are also used to ensure the security of messages sent from DHCT 333. The example shown in FIG. 4 is a forwarded purchase message (FPM). The forwarded purchase message is used for the interactive purchase of an instance of a service. One example of such a purchase is what is called impulse pay-per-view, or IPPV. In such a system, the beginning of an event, for example, a baseball game, is broadcast generally and customers can decide whether they want to see all of it. In that case, they must provide input to DHCT 333 that indicates that they wish to see the entire event. EMM manager 407 responds to the input by making the FPM and sending it to the entitlement agent so that the entitlement agent can charge the customer for the event and send an EMM 315 confirming that DHCT 333 may continue to decrypt the event. The information needed by the entitlement agent is forwarded entitlement information 417; to ensure the privacy of the customer, this information is encrypted using the 3DES algorithm with a key 420, as shown at 343, to produce encrypted forward entitlement information 419. The key 420 is composed of two 56-bit DES keys. The 3DES encryption operation is a sequence of three DES operations: encryption using the first DES key, decryption using the second DES key, and encryption using the first DES key Then key 420 is encrypted using the public key 335 of the entitlement agent and the sealed digest is made using the private key of DHCT 333. All of these parts together make up forwarded purchase message 421, which is addressed to the entitlement agent. (col. 12, lines 39-67)

Further, implementing the operation of encrypting the second encryption key *in the conditional access module* rather than elsewhere has particular advantages with respect to the use of metadata in the storage and retrieval of media programs. These advantages are further discussed with respect to claim 6 below. While claim 1 does not recite the use of metadata, claim 1 does recite functional features which enable the use of such metadata, providing further evidence of the patentability of claim 1.

For all of the foregoing reasons, the Applicants respectfully traverse the rejection of claim 1.

With Respect to Claim 2: Claim 2 recites:

> *The method of claim 1, wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of:*
> *decrypting the received access control information to produce the temporally-variant control data; and*
> *modifying the temporally variant control data to generate temporally-invariant control data.*

According to the Office Action, these features are disclosed as follows:

Update Entitlement Agent Properties

This EMM contains the values for EA fields 1516 of EAD 1409. EA administration EMM code 1317 reads EMM header 1113 to get the EAID for the EA to which the EMM is directed and simply sets fields 1516 in EAD 1409 for the EA from the EMM.

Non-Event Broadcast EMMs

Of the non-event broadcast EMMs, four types will be discussed here. These are Update MSK, Update Bit Map, Update List, and update combinations with MSK and list or bitmap. Those skilled in the art will be able to easily apply the principles explained below to EMMs that perform the functions indicated by the names of the other non-event broadcast EMMs. For example, the principles of digital EMMs can be applied to analog EMMs. There is a separate type of NVSC 1405 for each information type provided by the above non-event broadcast EMMs. FIG. 16 shows the contents of four of these types of NVSCs. Each NVSC type will be discussed together with the EMM that provides the information it contains.

Update MSK

The Update MSK EMM is used to send a new MSK for a set of services provided by the EA specified by the EMM. The new MSK and other information associated with the MSK are stored in MSK NVSC 1601 in list 1411 for EA information 1333 belonging to the EA specified by the EMM. Included in MSK NVSC 1601 is header 1502. Header 1502 specifies that NVSC 1601 is a MSK NVSC, gives the NVSC's name, and contains next element pointer 1507 to the next element in list 1411. The other fields contain information about the MSK. In the preferred embodiment, MSK 1608 has two 128-bit parts: the even MSK 1609 and the odd MSK 1611. Each part has two halves, i.e., a first half and second half, each of which has 56 key bits and 8 unused parity bits. The MSK 1608 is associated with a pair identifier 1603 for MSK 1608, an expiration date 1605 for MSK 1608, and a flag 1607 indicating whether the value of expiration date 1605 should be ignored. If the expiration date 1605 is not to be ignored, DHCTSE 627 will not use MSK 1608 to decrypt a control word after the expiration date. The identifier 1603 is per-EA, and consequently, a given EA may have one or more MSK NVSCs 1601 at any given time to store a plurality of different MSKs. Thus, conditional access system 601 not only permits separate security partitions for each EA, but also permits security partitions within an EA.

The Update MSK EMM header contains the EAID needed to locate EA information 1333 for the EA; the message contains the name of the NVSC that is to receive the MSK, a MSK pair selector which specifies a MSK pair ID for the MSK to be updated, a set of flags permitting the EA to selectively change MSK pair ID 1603, expiration date 1605, no expiration date 1607 and either half of MSK 1608, and the information needed to make the changes. At a maximum, the EMM contains a value for MSK pair ID 1603, a value for expiration date 1605, a value for no expiration date 1607, and values for even MSK 1609 and odd MSK 1611. EA MSK code 1319 processes the Update MSK EMM by locating EA Information 1333 for the EA identified by the EMM header's EAID, using the cell name to locate the proper NVSC, giving that NVSC the MSK type, and then writing to the MSK NVSC 1601 as required by the flags and the information in the EMM. This procedure is the same for both analog and digital Update MSK EMMs. The differences are in the EMM command code in EMM Header 1123 and NVSC type 1503. (col. 28, line 43 through col. 29, line 39)

The Applicants do not understand how the foregoing can be interpreted to disclose the features recited in claim 2. Absent further explanation of specifically where and how the modification step is disclosed, the Applicants must traverse.

With Respect to Claims 5 and 6: Claim 5 recites that "the access control information further comprises metadata describing at least one right for the program material", and claim 6 recites that

the second encryption key is generated at least in part from the metadata. According to the Office Action, this feature is disclosed as follows:

> Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107 to generate control word 117. Of course, a new control word is generated for each new ECM 107. (col. 4, lines 50-61)

The foregoing merely discloses that the control word (CW) is obtained from a message and authorization information (which may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch) stored in the set top box. It does not disclose using metadata *to generate* any key.

The use of metadata also highlights the inventive aspect of the Applicants' invention described in claim 1. The metadata is included in the access control information that is decrypted in the CAM, and in one embodiment, includes replay rights to the subject program material. Since it is advantageous to store the metadata in a hard drive for later comparison to the metadata stored in the IC card, the metadata (which is decrypted and available in the Applicant's CAM) should not be transmitted to an encryption module outside of the CAM for encryption, as this would expose the metadata (which, in one embodiment, defines replay rights) to compromise. The Applicants invention avoids this problem, because the metadata (after being used to generate the CP key or after augmenting the CP, depending on the embodiment) is not exposed to compromise and is only stored in an encrypted form. The encryption of the CP key *within* the CAM *where the metadata is also decrypted*, permits these advantages, while also allowing the metadata to be used for controlling replay.

With Respect to Claims 7-9: Claims 7-9 recites that steps (b)-(f) are performed in response to a pre-buy message. The referenced portion of the Akins reference (at col. 12, lines 39-67) discusses IPPV, but it does not specify or even remotely suggest that anything analogous to steps (b)-(f) of claim 1 be performed in response to that message. All that Akins discloses is that a different EMM is transmitted to the subscriber to the user, allowing the user to decode the program material. In no way is this analogous to steps (b)-(f).

With Respect to Claims 12-13: Nothing in the Akins reference discloses generating replay rights from metadata. Hence, claims 12-13 are allowable as well.

With Respect to Claim 17: As discussed above, the Akins reference discloses a conditional access module that decrypts the access control information to produce the first encryption key (see col. 21, lines 1-14), but while this module has encryption and decryption capabilities, it does not does not disclose the encryption of keys with another key. Instead, the encryption operations taking place in the DHCTSE are merely used for communications with the head end. As far as the Applicants can ascertain, none of these operations involve encrypting one key with another. If the Akins reference does in fact disclose such functionality, the Applicants would appreciate a specific citation to where in the Akins reference these features may be found.

With Respect to Claimed 18 and 27: Claims 18 and 27 recites additional features not disclosed in the Akins reference. For example, claim 18 recites a tuner that receives encrypted access control information and encrypted program material and other elements that are releasably communicatively coupleable with the conditional access module.

With Respect to Claims 19-26: Claims 19 and 26 are patentable for the reasons described above, for example, with respect to claims 7-9.

With Respect to Claims 28-42: Claims 28, 29, and 31-42 recite features similar to those of claims 1-16, and are patentable for the same reasons.

V. Dependent Claims

Dependent claims 2-16, 18-27, and 29-42 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VI. New Claims

New Claims 43-50 are presented for the first time in this Amendment. For the reasons described above, new claims 43-50 are patentable over the prior art of record, and the Applicants respectfully request the allowance of these claims as well.

VII. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

The DIRECTV Group, Inc.
RE / R11 / A109
P.O. Box 956
2250 E. Imperial Highway
El Segundo, CA 90245-0956
(310) 964-4615

By _____
Georgann S. Grunebach
Registration No.: 33,179
Attorneys for Applicant(s)

Date: January 20, 2005

Customer No. 020991